Espacenet

Bibliographic data: CN 1289974 (A)

Method and system for visiting several servers in www network by a user for registration once only

Publication date:	2001-04-04
Inventor(s):	GRANCOLLA M L [US]; LOUGH F [US]; WILLAMS M [US] +
Applicant(s):	URBAN GROUP DEV CT CORP [US] +
Classification:	- **International:** ***G06F21/00; H04L29/06;*** (IPC1-7): G06F15/163 - **European:** G06F21/00N5A2C; G06F21/00N5A2S; H04L29/06S8A; H04L29/06S8D
Application number:	CN20001030577 20000925
Priority number(s):	US19990155853P 19990924
Also published as:	• CN 1308870 (C) • EP 1089516 (A2) • EP 1089516 (A3) • EP 1089516 (B1) • DE 60031755 (T2) • more

Abstract not available for CN 1289974 (A)
Abstract of corresponding document: EP 1089516 (A2)

Methods and systems for single sign-on user access to multiple web servers are provided. A user is authenticated at a first web server (e.g., by user name and password). The first web server provides a web page to the user having a service selector (e.g., a hyperlink comprising the URL of a second web server offering the service indicated by the selector). When the user activates the service selector, the first web server constructs and transmits an encrypted authentication token (e.g., a cookie) from the first web server to a second web server via the user client. The first and second web servers share a sub-domain. The authentication token comprises an expiration time and is digitally signed by the first web server and is authenticated at the second web server. Upon authentication, the second web server allows the user to conduct a session at the second web server.

Last updated: 26.04.2011 Worldwide Database 5.7.22; 92p

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 15/163

[12]发明专利申请公开说明书

[21]申请号 00130577.8

[43]公开日 2001年4月4日

[11]公开号 CN 1289974A

[22]申请日 2000.9.25 [21]申请号 00130577.8
[30]优先权
[32]1999.9.24 [33]US [31]60/155,853
[71]申请人 城市集团发展中心有限公司
地址 美国加利福尼亚州
[72]发明人 迈克尔·L·格朗科拉 弗朗斯·洛
迈克尔·威廉姆斯 托尼·墨施恩
阿什维·杜什 约纳·江
扬克·潘

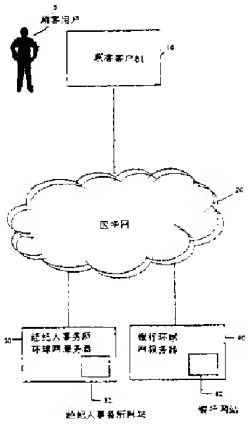
[74]专利代理机构 隆天国际专利商标代理有限公司
代理人 潘培坤 陈 红

权利要求书7页 说明书18页 附图页数4页

[54]发明名称 单次注册用户访问多个环球网服务器的方法和系统

[57]摘要

一种单次注册用户访问多个环球网服务器的方法和系统。在第一 个环球网用户鉴别用户的身份。第一个环球网服务器构造一个加密鉴 权权标,并从第一个环球网服务器发送给第二个环球网服务器。第一 个和第二个环球网服务器共享一个子域。这一鉴权权标包括一个截止 时间,并由第一个环球网服务器用数字方式签署,由第二个环球网服 务器鉴别。鉴别通过后,第二个环球网服务器允许用户跟第二个环球 网服务器对话。



ISSN1008-4274

00·10·08

权　利　要　求　书

1．一种单次注册用户访问多个环球网服务器的方法，其特征在于，包括下列步骤：

在第一个环球网服务器中鉴别用户身份；

从第一个环球网服务器向第二个环球网服务器发送一个加密鉴权权标，其中的鉴权权标包括一个截止时间，并由第一个环球网服务器进行数字签名；

在第二个环球网服务器里鉴别这一鉴权权标；和

允许这一用户在第二个环球网服务器里进行对话。

2．根据权利要求 1 的方法，其中第一个环球网服务器和第二个环球网服务器共享一个子域名。

3．根据权利要求 2 的方法，还包括只在截止时间还没有过的时候，在第二个环球网服务器中检查鉴权权标截止时间，并允许用户在第二个环球网服务器进行对话。

4．根据权利要求 3 的方法，其中的鉴权权标包括一个曲奇。

5．根据权利要求 4 的方法，其中从第一个环球网服务器向第二个环球网服务器发送加密鉴权权标包括从第一个环球网服务器向用户，然后从用户向第二个环球网服务器发送这一加密鉴权权标。

6．根据权利要求 5 的方法，其中在第一个环球网服务器里鉴别用户的身份包括接收用户名和口令。

7．根据权利要求 6 的方法，其中从第一个环球网服务器向第二个环球网服务器发送加密鉴权权标包括从第一个环球网服务器向用户的一台计算机发送这一鉴权权标；并从用户的计算机向第二个环球网服务器发送这一鉴权权标。

8．根据权利要求 7 的方法，其中第一个环球网服务器和第二个环球网服务器包括一群环球网服务器。

9．根据权利要求 8 的方法，其中在第二个环球网服务器中鉴别鉴权权标包括检查曲奇。

10．根据权利要求 9 的方法，还包括对鉴权权标进行 URL 编码。

11．根据权利要求 10 的方法，还包括在第二个环球网服务器中对鉴权权标进行 URL 译码。

12．根据权利要求 11 的方法，还包括为用户提供有一个服务选择器的一个网页。

13．根据权利要求 12 的方法，其中的服务选择器包括一个超级链接。

14．根据权利要求 13 的方法，其中的超级链接包括第二个环球网服务器的一个 URL 。

15．一种用户通过单次注册来访问一群环球网服务器的方法，其特征在于，包括以下步骤：

允许计算装置的用户通过该计算装置的环球网浏览器访问一群环球网服务器中的第一个环球网服务器；

第一个环球网服务器利用用户提供的鉴别信息鉴别用户的身份，该鉴别信息至少包括用户标识；

提示用户选择至少第二个环球服务器提供的功能；

接收用户对第二个环球网服务器提供的功能的选择；

第一个环球网服务器为这个用户产生一个鉴权权标，至少包括用户标识，以及一个预先确定的截止时间标记；

第一个环球网服务器用数字方式签署这一鉴权权标；

第一个环球网服务器将这一鉴权权标的域属性设置为共享的子域名；

第一个环球网服务器将数字签署过的鉴权权标发送给计算装置的环球网浏览器；

第一个环球网服务器将这一环球网服务器重新定向到第二个环球网服务器；

第一环球网浏览器将这一鉴权权标发送给第二个环球网服务器；

第二个环球网服务器将这一鉴权权标解密；

第二个环球网服务器检查鉴权权标中预先确定的截止时间；

如果是在这一预先确定的鉴权权标截止时间以前，就允许该用户跟第二个环球网服务器进行对话。

16．根据权利要求 15 的方法，还包括允许该用户跟第一个环球网服务器进行对话。

17．根据权利要求 16 的方法，其中第二个环球网服务器跟第一个环球网服务器共享一个子域。

18．根据权利要求 17 的方法，其中第一个环球网服务器以数字方式签署鉴权权标包括用公开密钥加密方式数字签署这一鉴权权标。

19．根据权利要求 18 的方法，还包括确认跟数字签名是否相同。

20．一种为多个环球网服务器单次注册的方法，包括：

从第一个服务器的一个用户接收登录数据；

为该用户提供一个服务选择器；

接收一个信号，说明该用户选择了这一服务选择器；

构造一个鉴权权标，该鉴权权标包括跟这个用户有关的简档数据；

加密和签署这一鉴权权标；

将这一用户重新定向到第二个服务器；

发送这一鉴权权标给该用户；

在第二个服务器里接收这一鉴权权标；

00·10·08

在第二个服务器里核实这一鉴权权标；和

允许该用户访问第二个服务器提供的一项服务。

21．根据权利要求 20 的方法，其中的鉴权权标还包括截止时间数据。

22．根据权利要求 21 的方法，其中的鉴权权标包括一个曲奇。

23．根据权利要求 22 的方法，其中的登录数据包括一个用户名和一个口令。

24．根据权利要求 23 的方法，其中的服务选择器包括一个超级链接。

25．一种单次注册用户访问多个环球网服务器的系统，其特征在于，包括：

在第一个环球网服务器鉴别用户身份的装置；

从第一个环球网服务器向第二个环球网服务器发送一个加密鉴权权标的装置，其中的鉴权权标包括一个截止时间，并被第一个环球网服务器以数字方式签名；

在第二个环球网服务器鉴别该鉴权权标的装置；和

允许该用户在第二个环球网服务器对话的装置。

26．根据权利要求 25 的系统，其中的第一个环球网服务器和第二个环球网服务器共享一个子域名。

27．根据权利要求 26 的系统，还包括在第二个环球网服务器内检查鉴权权标截止时间的装置。

28．根据权利要求 27 的系统，其中的鉴权权标包括一个曲奇。

29．根据权利要求 28 的系统，其中从第一个环球网服务器向第二个环球网服务器发送加密鉴权权标的装置包括从第一个环球网服务器向用户发送加密鉴权权标，然后从用户向第二个环球网服务器发送加密鉴权权标的装置。

30．根据权利要求 29 的系统，其中第一个环球网服务器鉴别用户身

份的装置包括接收用户名和口令的装置。

31．根据权利要求 30 的系统，其中从第一个环球网服务器向第二个环球网服务器发送加密鉴权权标的装置包括从第一个环球网服务器向用户的计算机发送鉴权权标的装置，以及从用户的计算机向第二个环球网服务器发送鉴权权标的装置。

32．根据权利要求 31 的系统，其中第一个环球网服务器和第二个环球网服务器包括一群环球网服务器。

33．根据权利要求 32 的系统，其中第二个环球网服务器鉴别鉴权权标的装置包括检查这一曲奇的装置。

34．根据权利要求 33 的系统，还包括对鉴权权标进行 URL 编码的装置。

35．根据权利要求 34 的系统，还包括在第二个环球网服务器那里对鉴权权标进行 URL 译码的装置。

36．根据权利要求 35 的系统，还包括提供有一个服务选择器的一个网页给用户的装置。

37．根据权利要求 36 的系统，其中的服务选择器包括一个超级链接。

38．根据权利要求 37 的系统，其中的超级链接包括第二个环球网服务器的一个 URL 。

39．一种单次注册用户访问一群环球网服务器的系统，其特征在于，包括：

允许计算装置前的用户通过该计算装置的一个环球网浏览器访问这一群环球网服务器中的一个环球网服务器的装置；

第一个环球网服务器利用用户提供的鉴别信息鉴别用户身份的装置，该信息至少包括一个用户标识；

提示用户选择通过至少第二个环球网服务器提供的一项功能的装置；

接收用户对第二个环球网服务器提供的功能的选择的装置；

第一个环球网服务器为该用户产生鉴权权标的装置，该鉴权权标至少包括用户的用户标识和预先确定的鉴权权标截止时间；

第一个环球网服务器以数字方式签署这一鉴权权标的装置；

第一个环球网服务器将这一鉴权权标的域属性设置为共享的子域名的装置；

第一个环球网服务器将数字签署过的鉴权权标发送给计算装置的环球网浏览器的装置；

第一个环球网服务器将这一环球网浏览器重新定向到第二个环球网服务器的装置；

这一环球网浏览器将这一鉴权权标发送给第二个环球网服务器的装置；

第二个环球网服务器将这一鉴权权标解密的装置；

第二个环球网服务器检查鉴权权标中预先确定的截止时间的装置；和

如果是在这一预先确定的鉴权权标截止时间以前，就允许该用户跟第二个环球网服务器进行对话的装置。

40．根据权利要求 39 的系统，还包括允许该用户跟第一个环球网服务器进行对话的装置。

41．根据权利要求 40 的系统，其中第二个环球网服务器跟第一个环球网服务器共享一个子域。

42．根据权利要求 41 的系统，其中第一个环球网服务器以数字方式签署鉴权权标的装置包括用公开密钥加密方式数字签署这一鉴权权标的装置。

43．根据权利要求 42 的系统，还包括确认跟数字签名是否相同的装置。

44．一种为多个环球网服务器单次注册的系统，包括：

从第一个服务器的一个用户接收登录数据的装置；

为该用户提供一个服务选择器的装置；

接收一个信号，说明该用户选择了这一服务选择器的装置；

构造一个鉴权权标，该鉴权权标包括跟这个用户有关的简档数据的装置；

加密和签署这一鉴权权标的装置；

将这一用户重新定向到第二个服务器的装置；

发送这一鉴权权标给该用户的装置；

在第二个服务器里接收这一鉴权权标的装置；

在第二个服务器里核实这一鉴权权标的装置；和

允许该用户访问第二个服务器提供的一项服务的装置。

45．根据权利要求 44 的系统，其中的鉴权权标还包括截止时间数据。

46．根据权利要求 45 的系统，其中的鉴权权标包括一个曲奇。

47．根据权利要求 46 的系统，其中的登录数据包括一个用户名和一个口令。

48．根据权利要求 47 的系统，其中的服务选择器包括一个超级链接。

00.10.03

说　明　书

单次注册用户访问多个环球网服务器的方法和系统

总的来说，本发明涉及电子商务领域。更具体地说，本发明的实施方案涉及单次注册用户访问多个环球网服务器的一种方法和系统。

本专利申请要求享受共同未决的第 60/155853 号美国临时专利申请的优先权，该申请的标题是“单次注册（ single sign-on ）用户访问一群（ a federation of ）环球网服务器的方法和系统”，于 1999 年 9 月 24 日提交，这里将它全部引入作为参考。

在许多情况下，一个实体或者一组实体，比方说有银行服务、经纪服务等等的全球金融机构，希望将不同全球网应用服务器的功能资源组合起来，以便为这一个实体或者这一组实体的顾客提供集成功能服务。这样一个实体或者一组实体可能会希望让它们的顾客只通过一次注册，鉴别一次他们的身份，便能访问这样的集成功能，获得不同的服务，这些不同的服务可能是由这一组实体中一些实体的不同服务器提供的，也可能是由这一组实体的一些服务器提供的，以及例如，由第三方实体的服务器提供的。

在这种情况下，这一实体或者这一组实体可能希望通过环球网浏览器，为这一顾客提供一组服务，这一组服务由不同的环球网应用程序服务器提供。这些应用程序服务器可以采用不同的平台，比方说一个 UNIX 平台、一个 NT 平台或者某种其它类型的平台。这一平台可能已经由这一组实体中不同的组织建造，或者这一平台有可能是由第三方提供商提供的。不管是在哪种情况下，都有一个基本的问题，那就是如何让顾客只注册一次，然后就能将这一顾客重新定向到这些不同的服务器，而不需

要这个顾客在他或她每次访问一个不同的服务器时都要注册。

传统的产品想要解决这一问题是有缺陷的，例如，在性能和成本方面都有缺陷。在这样一些产品中，必须返回到一个中央资源去。其它的这种产品不支持跨越管理边界或者因特网区域边界。因此需要一种方法和系统，用于单次注册用户能够访问多个环球网服务器，比方说共享一个子域的一群环球网服务器，它能克服这些缺点，并能提供其它优点。

本发明提供一些方法和系统，用于单次注册用户访问多个环球网服务器，比方说共享子域的一群环球网服务器。在一个实施方案中，（例如通过用户名和口令）在第一个环球网服务器上鉴别用户的身份。这第一个环球网服务器提供网页给用户，上面有一个服务选择器（例如一个超级链接，它包括第二个环球网服务器的 URL，这第二个环球网服务器提供选择器指明的服务）。在用户激活选择器的时候，第一个环球网服务器构造并以数字方式签署一个加密鉴权权标（authentication token）（例如一个曲奇（cookie）），并通过用户客户机，从第一个环球网服务器向第二个环球网服务器发送这个加密鉴权权标。采用 ULR 编码来加密和签署鉴权权标。第一个和第二个环球网服务器共享一个子域。这个鉴权权标包括一个截止时间。在第二个环球网服务器内，采用 URL 译码方式对这一个鉴权权标进行检查和鉴权。在鉴权的时候，如果没有超过截止时间，第二个环球网服务器就允许用户跟第二个环球网服务器进行对话。

在另一个实施方案里，提供了一种方法，用于单次注册用户访问一群环球网服务器，比方说共享一个子域的第一个环球网服务器和第二个环球网服务器。在一个实施方案里，该方法包括让用户在一个计算装置上通过该计算装置的环球网浏览器，访问这一群环球网服务器的第一个环球网服务器，这第一个环球网服务器用用户提供的鉴权信息对用户进

行鉴权，这些鉴权信息至少包括一个用户标识，并让用户在这第一个环球网服务器上进行对话。在对话的过程中，第一个环球网服务器执行一项功能，提示用户选择通过至少第二个环球网服务器提供的一项功能，并接收用户对通过第二个环球网服务器提供的功能的一个选择。在收到选择的时候，第一个环球网服务器为这一个用户生成一个鉴权权标，该鉴权权标至少包括用户的标识，还有一个由第一个环球网服务器预先确定的权标截止时间，由第一个环球网服务器以数字方式签署（例如通过公钥加密）这一鉴权权标。一个实施方案还包括由第一个环球网服务器用共享的子域名使鉴权权标的域属性有效，由第一个环球网服务器发送这一经过数字签署的鉴权权标给这一计算装置的环球网浏览器，第一个环球网服务器将这一环球网浏览器重新定向到第二个环球网服务器，并由环球网浏览器发送这一鉴权权标给第二个环球网服务器。第二个环球网服务器对这一鉴权权标解密，跟第一个环球网服务器的数字签名进行比较，第二个环球网服务器检查鉴权权标里预先确定的截止时间，如果没有超过预先确定的权标截止时间，就允许用户跟第二个环球网服务器对话。

在另一个实施方案里，单次注册就能使用多个环球网服务器的一种方法，包括在第一个服务器里接收用户的数据，为用户提供一个服务选择器，接收一个标志，该标志说明用户选择了这一服务选择器，构造一个鉴权权标，这个鉴权权标包括跟用户有关的一个简档数据，加密并签署这一鉴权权标，将用户重新定向到第二个服务器，发送这一鉴权权标给用户，第二个服务器接收这一鉴权权标，第二个服务器核实这一鉴权权标，并允许这个用户访问第二个服务器提供的服务。在这样一个实施方案里，鉴权权标包括一个曲奇，还包括截止时间数据。

本发明的一个特征和优点是，提供一种方法和系统，用于单次注册

用户访问一群环球网服务器，该系统和方法允许已经在一个环球网网站鉴权的用户，比方说已经在一个金融机构的一个环球网网站鉴权的用户，能够访问，例如，一个服务提供商的环球网网站，而不需要通过提供有效用户名和口令重新鉴权。

为了实现上述特征和优点以及其它特征和优点，本发明的一个实施方案提供一种方法和系统，它能使单次注册用户访问一群环球网服务器，允许用户在一个实体的环球网站点服务器上鉴权，选择一个服务提供商的 URL ，并由这个实体的环球网站点服务器将一个鉴权权标传递给一个服务提供商的服务器，这个鉴权权标包括足够的信息，用于让服务提供商的服务器，例如，能够将这个用户识别为有效的服务提供商用户，并为该用户提供顾客专用信息。

本发明其它的目的、优点和新特征将部分地在下面的说明里介绍，通过以下说明使本领域里的技术人员更加清楚，或者能够通过实施本发明来了解。

图 1 说明了本发明一个系统的一个实施方案。

图 2 给出了一个流程图，它说明图 1 所示系统实现的本发明中的过程。

图 3 给出了跟图 1 所示系统的环球网服务器有关的网页的一个形象说明。

图 4 给出了一个流程图，它说明图 1 所示系统实现的本发明的另一个过程。

图 1 说明了本发明一个系统的一个实施方案。一个经纪人事务所环球网服务器（ BFWS ） 30 包括一个经纪人事务所网站 32 。这个经纪人事务所环球网服务器 30 （跟经纪人事务所网站 32 一样）跟因特网 20 进行通信。同样，一个银行环球网服务器 40 包括一个银行网站 42 。这个银

行环球网服务器（BWS）40（以及银行网站 42）也在跟因特网 20 进行通信。图中画出了这个经纪人事务所和这个银行的一个顾客 5。顾客 5 有一个用户名和口令，用来访问经纪人事务所网站 32 和银行网站 42。这个顾客的个人计算机 10 有一个环球网浏览器，比方说微软的因特网浏览器或者网景公司的导航器（一个客户程序），也在跟因特网 20 通信。顾客 5 用顾客的个人计算机和浏览器 10 通过因特网跟环球网服务器 30、40 通信。在这里，顾客这个术语在许多情况下都用来表示顾客使用的客户机 10。除了网络通信设备等等以外，这个经纪人事务所环球网服务器 30 和银行服务器 40 都包括一些程序，用来执行这里描述的功能。

图 2 给出了图 1 所示系统执行的步骤的一个流程图。顾客 5 将顾客的浏览器指向经纪人事务所网站 32。顾客 5 用顾客在经纪人事务所网站 32 上正确的用户名字（或者用户标识）和口令登录到这一经纪人事务所网站 32，然后由经纪人事务所环球网服务器 30 鉴权。一旦顾客登录到经纪人事务所网站 32，网站 32 就从网站 32 为顾客 5 提供一个欢迎页。一旦登录进来以后，顾客 5 就可以检查顾客的经纪账号信息、有价证券、投资信息等等。

图 3 给出了图 1 所示系统的一个图形描述，包括顾客登录进入经纪人事务所网站 30 以后从经纪人事务所网站 30 提供给顾客的欢迎页 100。图 3 中说明的欢迎页 100 包括一个服务选择器，它的形式是标为“记账支付” 102 的一个超级链接。经纪人事务所网站使它的顾客能够支付账单。

再一次参考图 2，顾客 5 通过点击“记账支付”超级链接 102 请求进行记账支付 50。经纪人事务所环球网服务器 30 自己并不执行记账支付过程，但是服务器 30 中的程序知道银行环球网服务器 40 执行这样一个过程。超级链接 102 包括银行网站 42 的 URL。检测到记账支付的请求

时，经纪人事务所服务器 30 构造一个鉴权权标 52 。鉴权权标包括一个对象（或者数据），可以在协作的服务器之间传递。鉴权权标一个实施方案的一项功能是将必需的信息从主（或者第一个）服务器传递给辅助（或者第二个）服务器，让辅助服务器跳过注册过程，如果不这样，这一注册过程就是必须的。一旦主服务器为用户建立起一个对话，从主服务器接收有效鉴权权标的协作的辅助服务器就能建立对话，而不用用户再一次注册。

在图 1 所示的实施方案里，经纪人事务所环球网服务器 30 构造一个鉴权权标（或者一个访问权标），其中包括用户标识数据（或者简档数据）和截止时间数据（权标截止时间） 52 。简档数据包括用户标识数据，用户标识数据包括顾客的识别号，该识别号向辅助服务器唯一地说明用户的身份。在图示实施方案里，该权标还包括这个顾客的一个账目清单。截止时间数据包括一些数据，说明超过这一时间以后鉴权权标就失效。在给出的实施方案里，时间是格林威治平均时间（ GMT ）。在其它的实施方案里，时间可以是世界时。截止时间可以由主服务器在任何时候设置，尽管在多数实施方案里，从产生鉴权权标的时刻算起，这个截止时间是一个相对短的时间，例如，三分钟到二十分钟。在给出的实施方案里，截止时间被设置成从产生鉴权权标的时刻开始过十五分钟。注意，交换这种鉴权权标的服务器保持正确或者同步的时钟是非常重要的。截止时间的使用是产生一个一次有效、容易失效的权标。

在给出的实施方案中，构造的鉴权权标包括一个曲奇，其中包括顾客 5 的简档数据和从权标产生时刻开始算起的十五分钟的截止时间。鉴权消息还可以包括 URL 字符串或者能够在服务器之间传递的其它数据。顾客的简档数据包括顾客 5 的顾客识别号。经纪人事务所环球网服务器 30 包括一个数据存储系统（例如一个硬盘驱动器），其中有跟经纪人事

务所环球网服务器 30 的顾客使用的登录用户名有关的顾客识别号。这些号码由服务器 30 、 40 的管理员事先协商好。在给出的实施方案里，一个顾客跟一个顾客识别号相关联。在这一实施方案中，当顾客请求进行记账支付 50 的时候，服务器 30 从数据存储系统中检索出顾客 5 的识别号。检索出来的这一顾客识别号被用于用来构造曲奇 52 的简档数据中。

在另一个实施方案里，各种顾客识别号跟各种辅助服务器相关联。当顾客请求一个辅助站点提供的服务（或者要转移到一个辅助站点）时，主服务器检测到这一请求，确定辅助站点，并从数据存储系统中检索出跟顾客要被连接过去以获得记账支付服务的这一辅助站点有关的、发出请求的顾客的顾客识别号。

再一次参考图 2 ，服务器 30 还选择辅助服务器接收方名称 54 。服务器 30 通过检查顾客发出的请求，确定处理这一请求的合适的辅助服务器的名称/地址来做到这一点。在给出的实施方案里，服务器 30 检查顾客发出的“记账支付”请求。在当前实施方案里，这一检查包括确定跟“记账支付”超级链接有关的统一资源地址（ URL ）。跟欢迎页 100 有关的网页文件包括跟“记账支付”超级链接有关的 URL ，服务器 30 选择这一 URL 。

然后，服务器 30 签署并加密曲奇 56 。服务器 30 在曲奇 56 上签上经纪人事务所 30 的数字签名。最好是，服务器 30 包括公开密钥加密软件，该软件能够在应用程序和服务器之间进行加密、数字签署和鉴别电子交易。在给出的实施方案里， Entrust/PKT 5.0 软件包，以及它的应用程序接口（ API ）库，从德克萨斯 Plano 的 Entrust 技术有限公司可以获得它们，它们被用于利用公开密钥加密系统签署这一曲奇。在给出的实施方案里，使用的加密器是 Triple DES （数据加密标准）加密算法系统，加密以后的曲奇采用保密性增强型邮件（ PEM ）报头，并利用安

全散列算法（ SHA-1 ）来产生签字的消息摘要（或者散列值）。这里的 Triple DES 系统用于加密鉴权权标（曲奇），还包括一个 PEM 报头和一个 SHA-1 摘要。

用于曲奇、跟服务器 30 有关的数字签名（以签名加密字符串的形式）使得辅助服务器能够核实这一鉴权权标是由经纪人事务所服务器 30 产生的。此外，这一签名使得辅助服务器能够检测出来这一鉴权权标是否被改动或者被破坏。这一数字签名由服务器 30 来完成和加密。

在给出的实施方案里，这一曲奇用响应页中的一个标题项被产生并保留在用户 5 的浏览器 10 中，这一标题项的结构如下：设置曲奇；名称=值；截止时间=日期和时间；域=域名；路径=路径；安全。其中的路径值包括一个具体的路径，域名值最好是一个公用子域（下面将进一步讨论）。在一个实施方案里，鉴权权标（曲奇）是不稳定的，不会写入顾客客户机 10 的磁盘。在这样一个实施方案里，不需要失效值，曲奇会在接收到以后被接收它的服务器立即删去。

本发明一个实施方案中包括曲奇结构的字符串的一个实例如下：

VER|1EXPDT|19990505132540||CT\CUST|AF|EXIST||CID|576001000560050234||

FCID|0||TA|2||ANM|0010000001||RTN|099||ANA|我妻子的检验||ab|237600||ANM|0010000002||RTN009||ANA|我的检验||AB|24556 。该实例的格式如下：标签 1 标签值 1 标签 2 标签值 2 标签 3 标签值 3 ……

应该指出：具体的标签和标签值可能会随着应用需要而变化，比方说随目的地服务器的要求而变化。

在给出的实例中，标签、它们的值以及说明在下表中给出：

标签	标签值	说明
VER	1	使用的曲奇系统的版本（当前版本是 1）
EXPDT	日期/时间	鉴权权标失效的 ASCII GMT 日期和时间，格式是： CCYYMMDDHHMMSS
CT	CUST FC	顾客类型。 CUST=老主顾。 FC=顾客代表。用于激活只查看模式。
AF	新的/存在	新顾客或者已经存在的顾客标志
CID	整数	顾客识别号
FCID	字母数字	顾客服务代表的识别号。如果这个顾客是一个老主顾，就不将 FCID 置位（也就是将它设置成 0）
TA	整数	顾客账号的总个数
ANM	整数	账号号码
RTN	整数	路由选择支票交换号码—到 prod-type-ed 的图
ANA	字母数字	账号别名
AB	整数	账号结余，以分为单位（也就是说 $10.50=1050）

在上述实施方案中，标签的顺序没有意义，除了 ANM、 ANA、 AB 以外，它们被看成一个多元组，放在一起，就象前面说明的一样。还有，在所述实施方案中， VER、 EXPDT 和 CT 是必须的标签。可以用于其它实施方案的其它标签包括： AG（雇用用户的代理或者公司的名称）、 FNAM（用户的名）和 LNAM （用户的姓）。

AF 标签使银行服务器 40 能够判断是否应当向一个交易处理系统

（ TPS ）发去一则“启动用户”消息。如果经纪人事务所环球网服务器 30 不能确定一个顾客是新顾客还是已经在 GTPS 中登记过，那么，服务器 30 最好将 AF 标签设置成新的。另外，说明的经纪人事务所环球网服务器 30 假设所有账号都属于“检验（ Checking ）”类型，并将在确定了的 RTN 值的基础之上设置产品类型。

然后，经纪人事务所服务器 30 对构成的曲奇 58 进行 URL 编码（也叫做 URLEncode ）。在对曲奇进行 URL 编码的过程中，经纪人事务所环球网服务器基本上将前面讨论过的格式化的字符串转换成上述 URL 编码格式。在一个实施方案里， URL 编码用 URL 转义句法对这一字符串编码，这一 URL 转义句法包括一个三字符字符串（%nn ），具体说明一个字符的十六进制码。这一句法用于隐藏一些字符，如果不隐藏这些字符，当它们用于 URL 时可能会是有意义的。经纪人事务所环球网服务器 30 所进行的 URL 编码 58 产生一个编过码、签过字和加过密的字符串，适合于写入一个曲奇中，这样一个字符串被服务器 30 包括在构造的曲奇中。

然后，经纪人事务所服务器 30 在设置曲奇报头中发送有 URL 编码曲奇（鉴权权标）的一个重新定向命令（或者重新定向页）给顾客客户机 60 。这一重新定向命令包括跟“记账支付” 42 有关的网站的 URL 。顾客客户机 10 收到这一重新定向命令和经纪人环球网服务器 30 构造的经过了 URL 编码的曲奇。

顾客的客户机 10 通过因特网 20 跟银行网站 42 连接，并将这一曲奇发送给银行环球网服务器 62 。在所示实施方案中，鉴权权标在加密套接字协议层（ SSL ）对话中发送。还有，在所示实施方案中，收到重新定向命令时，顾客客户机 10 打开第二个浏览器窗口，请求下载环球网服务器 42 的 URL 处的主页（或者 URL 指定的页），从银行环球网服务器 40 接收网站 42 的这一页，并在窗口中显示这一页。这样一个窗口 110 和页

的一个实施方案在图 3 里说明。顾客客户机 10 从经纪人事务所环球网服务器 30 收到的曲奇被顾客客户机 10 发送给银行环球网服务器 40 。

银行环球网服务器 40 从顾客客户机 10 那里接收曲奇。银行环球网服务器 40 将经纪人事务所环球网服务器 30 编码、签字和加密，放进曲奇的字符串译码，得到签过字、加过密的字符串 64 。这一译码采用的是给出的实施方案中的 URL 译码（或者 URLDecode ）方法。在所示实施方案中，采用了 URL 译码将曲奇中 URL 编码的字符串转换成普通 ASCII ，供银行环球网服务器 40 检查。在此之前银行环球网服务器 40 和经纪人事务所环球网服务器 30 交换过公开密钥-保密密钥解密信息。

一旦这一字符串被译码，银行环球网服务器 40 就对曲奇 66 （包括现在译码的签过字的加密字符串）进行解密和核实。在所示实施方案里，软件包括公开密钥加密软件，它能在应用程序和服务器之间对电子交易进行解密和鉴权，并由银行环球网服务器 40 用来这样做。这种软件的一个实例是 Entrust/PKT 5.0 软件包，以及它的应用程序接口（ API ）库，可以从德克萨斯 Plano 的 Entrust 技术有限公司获得。

利用这里介绍的软件，银行环球网服务器 40 判断曲奇中的数字签名是否正确 68 。如果这一签名不正确，银行环球网服务器 40 就拒绝这一注册，并将顾客客户机 10 重新定向到经纪人事务所环球网服务器 30 的--个网页上，说明由于失败的注册尝试 72 而发生了错误，注册失败 70 。在另一个实施方案里，如果这一签字不正确，银行环球网服务器 40 就拒绝注册，并发送一个网页给顾客的客户机 10 ，说明发生了错误，注册失败。在一个实施方案里，如果签字不正确，银行环球网服务器 40 也发送一则消息给经纪人事务所网站 30 ，例如一则电子邮件消息，说明这一操作失败。

如果这一签字正确，银行环球网服务器 40 就检查曲奇 74 的许可证

（CA）。服务器 40 比较曲奇的 CA 名（也就是预期的 CA 名使用的 CA，就象银行环球网服务器 40 里一个注册文件里记录的一样）。如果 CA 名不是预期的那一个，银行环球网服务器 40 就将顾客应用程序 10 重新定向到经纪人事务所环球网服务器 70 的一个出错页上去，注册尝试失败 72，就象前面介绍过的一样。

如果这一 CA 名是预期的 CA 名，那么，银行环球网服务器 30 下一步就检查发送方的名称是否正确 76。这样做的时候，银行环球网服务器 30 跟曲奇有关的普通名称（CN）（也就是正在证明的名称—经纪人事务所环球网服务器 30 使用的名称）是否是一个得到了认可的名称。在做这一判断的时候，银行环球网服务器 40 将跟这一曲奇有关的 CN 跟银行环球网服务器 40 中一个数据记录中一个文件里保存的授权名称进行比较。如果这一 CN 不是预期的那一个，银行环球网服务器 40 就将顾客应用程序 10 重新定向到经纪人事务所环球网服务器 70 的一个出错页去，注册尝试失败 72，就象前面介绍过的一样。

如果这一 CN 正确，也就是说，如果这一 CN 是一个被许可的名称，银行环球网服务器 40 就从曲奇中提取简档数据并开始记账支付对话 78。在所示实施方案里，服务器 40 分析跟曲奇有关的普通文字数据（普通文字指的是没有加密的信息）78，并检查曲奇中的截止时间（没有画出）。如果已经过了截止时间，银行环球网服务器 40 就将顾客应用程序 10 重新定向到经纪人事务所环球网服务器 70 上的一个出错页去，这一注册尝试失败 72，就象前面介绍过的一样。这些普通文字数据包括简档数据（例如顾客识别号）。如果截止时间还没过，环球网服务器 40 就通过发送图 3 所示的银行网站 42 的网页 110 给顾客客户机，用这一对话和简档数据 78 开始记账支付对话，这一注册是成功的 80。顾客客户机 10 收到这一网页 100，并跟银行服务器 40 继续这一记账支付对话。然后在一

个实施方案里，环球网服务器 40 将这一鉴权权标（曲奇）丢弃或者销毁。

在另一个实施方案里，系统反映跟用户的雇员有关的一项服务。这样一个实施方案在图 4 里说明。在图 4 所示的实施方案里，总的来说这一可选实施方案的过程跟上面讨论过的一样，以下讨论的内容例外。所示实施方案采用一个主服务器，它包括一个有一个中心网站（没有画出）的一个中心环球网服务器。这一中心网站包括这样一个网站，在那里，顾客客户机 10 可以通过点击超级链接请求各种服务。

参考图 4，顾客 5 在中心网站 49 那里注册，过程 150 、 152 、 154 、 156 、 158 、 160 、 162 、 164 、 166 、 168 、 170 、 174 按照图 3 所示步骤 50 、 52 、 54 、 56 、 58 、 60 、 62 、 64 、 66 、 68 、 70 、 74 中的方式继续下去，中心环球网服务器用作主服务器（在图 2 所示的实施方案里，经纪人环球网服务器用作主环球网服务器），直到进入示为 77 的步骤。主服务器在曲奇中包括以下额外的标签： AG（雇用这一用户的代理或者公司名称）、 FNAM （用户的名）和 LNAM （用户的性）。图 4 中提到的服务提供商包括辅助服务器，在所示实施方案里，包括银行环球网服务器 40 。在银行环球网服务器 40 认定发送方的 CA 正确以后，环球网服务器 40 就判断该顾客/用户的雇主是否已经在辅助服务器（银行环球网服务器 40 ） 77 那里的服务提供商那里注册。银行环球网服务器 40 包括一个数据库，其中包括一个雇主清单，这些雇主在银行环球网服务器 40 提供的服务那里注过册。环球网服务器 40 将 AG 标签中的代理或者公司名称跟这一个雇主清单比较。如果这一 AG 标签中的名称不在这个清单里，环球网服务器 40 就因为错误的 URL 70 将顾客的客户机 10 重新定向到中心网站。

如果 AG 标签里的名称在这一清单上，环球网服务器 40 就通过提取曲奇中的简档数据继续这一过程，开始记账支付对话 78 。在银行环球网

服务器 40 从曲奇提取出简档数据并开始记账支付对话 78 以后，服务器 40 检查跟这一服务器 40 有关的一个数据库（没有画出），该数据库包括数据，反映以前注册过或者使用过服务器 40 提供的服务的用户。如果曲奇反映的用户存在（也就是说，以前注册过或者使用过服务器 40 提供的服务），环球网服务器 40 就检索以前被选做用户的默认网页的默认网页，并发送这一默认网页给顾客客户机 83，然后，顾客客户机 10 就可以继续记账支付对话 80。

如果这一曲奇反映的用户不存在（也就是说，数据库没有反映用户以前注册过或者使用过服务器 40 提供的服务），环球网服务器 40 就用这一标签信息产生一个用户标识，包括 AG、FNAM 和 LNAM 标签信息，并将这一用户标识存入一个数据库里。然后，服务器 40 取出一个预先指定的默认网页，并发送这一网页给顾客客户机 83。这一预先指定的默认网页包括一个预先指定的网页，给跟 AG 标签说明的代理/公司有关的用户。然后，顾客客户机 10 就可以继续记账支付对话 80。

辅助服务器被用于本发明的一个实施方案。在另外一个实施方案里，采用了多个主服务器。像这里介绍的一样，共享注册和其它信息的一个或者多个主服务器和一个或者多个辅助服务器构成的一组可以叫做一“群”服务器（a “federation” of servers）。

在这里给出的实施方案中，采用了数字证书生成软件程序来产生证书。这种软件的一个实例是 Entrust Solo 4.0 版软件包，可以从德克萨斯 Plano 的 Entrust 技术有限公司获得，在本发明的一个实施方案中采用多个辅助服务器时，这些辅助服务器会使用同样的简档（在服务器能够鉴权之前包括证书所需要的信息的一个文件）。还有，简档里的 CN 名称最好跟辅助服务器的通用主机名相同。

在一些实施方案里，采用了多个辅助服务器。主服务器可以在所有

主机上使用相同的简档，或者每一个主机都可以使用一个不同的简档。跟辅助服务器一样，每一个主服务器都采用证书。

在一个实施方案里，在它们自己之间共享不同机构维护的信息的服务器之间，使用一个共享的域，以便简化信息的共享。在这样一个实施方案里，建立一个子域或者将一个子域指定为共同的子域，鉴权权标的域属性（例如共享的曲奇）被指定为共同的子域，并在协作机构的 DNS 名称服务器里增加一个“转发 IP （因特网协议）指针”。

例如，主服务器设置一个曲奇子域 xxxx.yyyy.com （其中 yyyy.com 包括主服务器的域名）。利用“尾部匹配”，所有域尾部是“ yyyy.com ”的主机都共享这些曲奇。当服务器在用户计算机上搜索曲奇清单寻找有效或者可用的曲奇时，服务器将曲奇的域属性跟主机的因特网域名进行比较。如果尾部相同，那么这一曲奇就开始路径匹配检查，看它是否应当发送。“尾部匹配”指的是用域属性的尾部跟主机完整的有效域名的尾部进行比较。例如，“ xxxx.com ”的域属性跟主机名“ yyyy.xxxx.com ”和“ zzzz.yyyy.xxxx.com ”相同。例如，用户打交道的主服务器的域名是 qqqq.yyyy.com ，而辅助服务器的域名则是 ssss.rrrr.yyyy.com ，它们可以在这样一个实施方案中共享曲奇。在一个实施方案里，跟主服务器有关的域名服务器里的 IP 指针或者（ 1 ）将辅助服务器域（ ssss.rrrr.yyyy.com ）映射到跟辅助服务器有关的一个预先指定的 IP 地址；或者（ 2 ）委派区域 “ rrrr ”给跟辅助服务器有关的一个 DNS 名称服务器，来解决这一问题。

如上所述，本发明的某些实施方案采用 URL 编码和 URL 译码。下面是一段用微软 C++ 6.0 编写的代码，这段代码说明的是一个服务器进行 URL 编码的一个实例：

```
//
// URL 编码将一些字符转换成%xx 格式，用于
//在 URL 中发送或者写入一个曲奇
//
void URLEncode ( BYTE* szDecoded, BYTE* szEncoded )
    {
        BYTE* pszInPtr = szDecoded;
        BYTE* pszOutPtr = szEncoded;
        BYTE inch;
        while (( inch = *pszInPtr++ ) !='\')
          {
            if (    ( inch < 32 )  ||( inch > 127 ) ||
                  ( inch == '=' )  ||  ( inch == '?' ) ||
                  ( inch == '&' )  ||  ( inch == '+' ) ||
                  ( inch == '%' )  ||  ( inch == '-' ) ||
                  ( inch == ':' )  ||  ( inch == ':' ) ||
                  ( inch == ',' ) )
          {
            *pszOutPtr++ = '%';
            sprintf((char*)pszOutPtr, "%02x", inch);
            pszOutPtr += 2;
          }
          else
            *pszOutPtr ++= inch;
          }
```

```
                *pszOutPtr ++= '\0\';;
        }
```

下面的代码段说明了服务器进行的 URL 译码：

```
//
// URL 译码将%xx 格式的字符转换回它们的 ASCII 值
//
void URLDecode (BYTE* szEncoded, BYTE* szDecoded )
{
     BYTE* pszInPtr = szEncoded;
     BYTE* pszInPtr = szEncoded;
     int   inch;

     while (( inch = *pszIntPtr++)     != '\0')
     {
          if ( inch ='%' )
               *pszOutPtr ++=(unHex ( pszInPtr ++) << 4 ) +
                              unHex(*pszInPtr++ );
          else
               *pszOutPtr ++= inch;
     }
     *pszOutPtr ++= '\0';
}
int unHex ( BYTE hexChar )
{
     if (( hexChar >='0' ) && (hexChar <= '9' ))
```

```
            return hexChar - '0';
        if (( hexChar >='a' ) && (hexChar <= 'f' ))
            return hexChar - 'a' + 10;
        if (( hexChar >='A' ) && (hexChar <= 'F' ))
            return hexChar - 'A' + 10;
        return 0;
    }
```

本领域里的技术人员会认识到，有各种代码段可以用于执行这些步骤。此外，还可以采用各种编程语言。

已经介绍了本发明的各种实施方案，用这些实施方案来达到本发明的各种目的。应当认识到，这些实施方案只是用于说明本发明的原理。对本领域里的技术人员而言，对本发明的各种修改和改进均属于本发明的实质和范围。

说　明　书　附　图

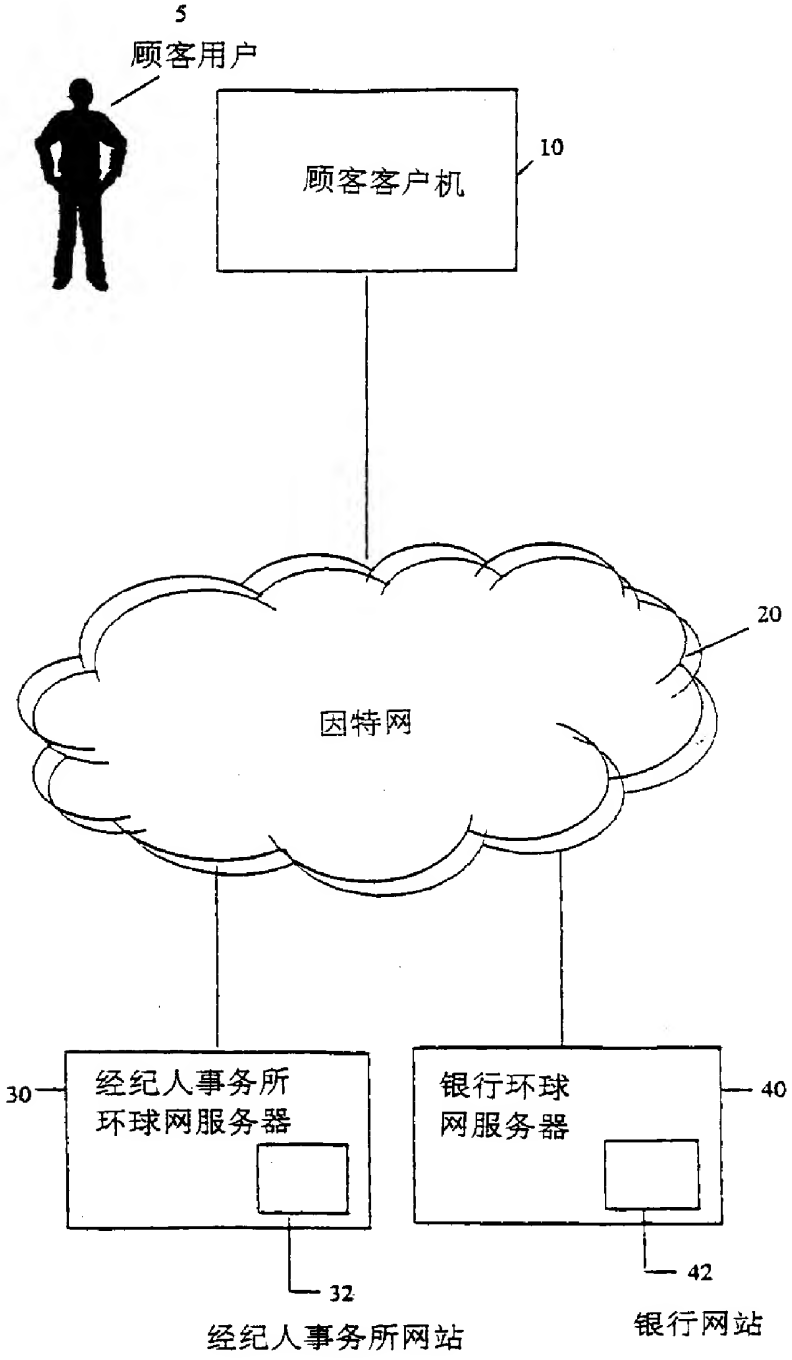

5
顾客用户
顾客客户机
10
因特网
20
经纪人事务所
环球网服务器
30
32
经纪人事务所网站
银行环球
网服务器
40
42
银行网站

图 1

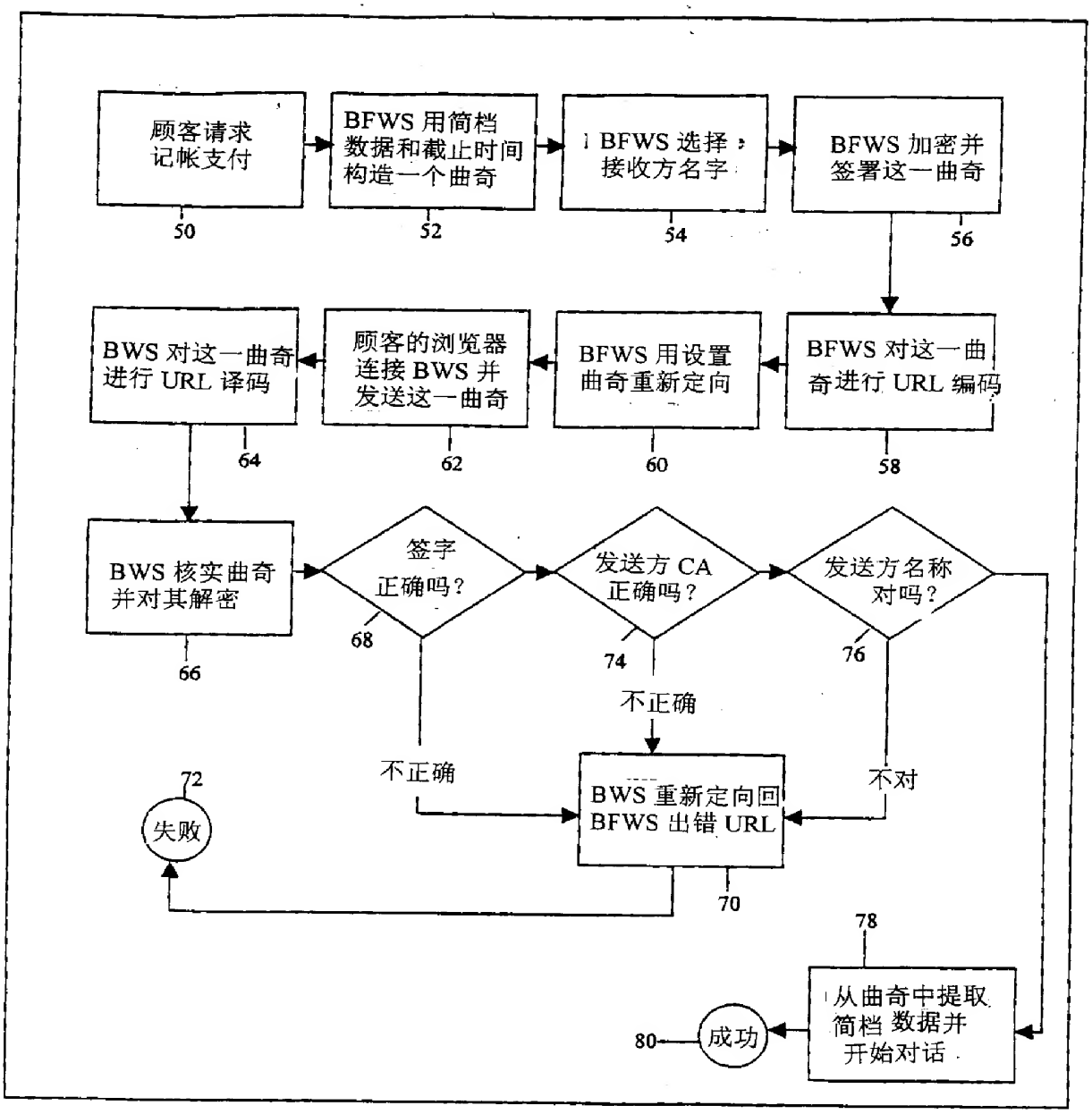
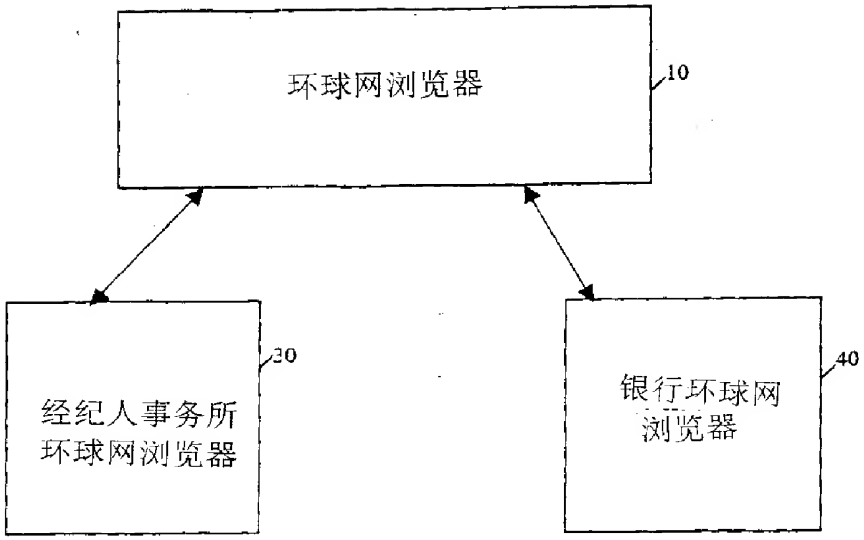
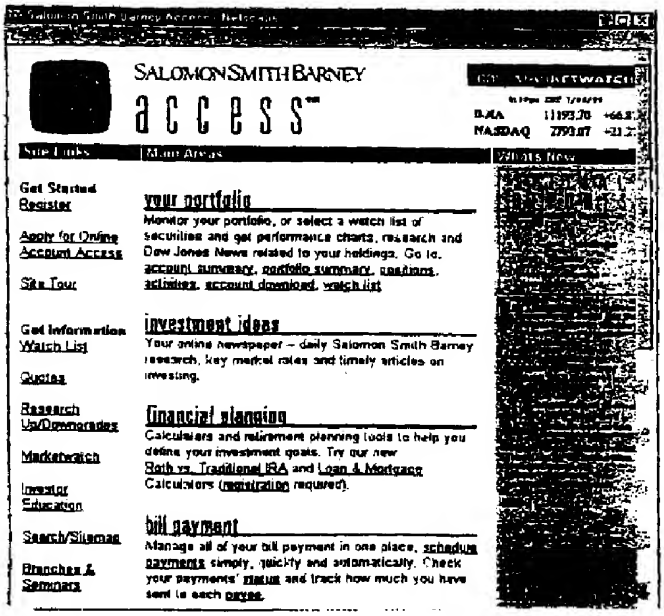

顾客请求
记帐支付
50
BFWS 用简档
数据和截止时间
构造一个曲奇
52
BFWS 选择
接收方名字
54
BFWS 加密并
签署这一曲奇
56
BFWS 对这一曲
奇进行 URL 编码
58
BFWS 用设置
曲奇重新定向
60
顾客的浏览器
连接 BWS 并
发送这一曲奇
62
BWS 对这一曲奇
进行 URL 译码
64
BWS 核实曲奇
并对其解密
66
签字
正确吗？
68
发送方 CA
正确吗？
74
发送方名称
对吗？
76
不正确
不正确
不对
72
失败
BWS 重新定向回
BFWS 出错 URL
70
78
从曲奇中提取
简档 数据并
开始对话
80
成功

图 2


环球网浏览器
10
经纪人事务所
环球网浏览器
20
银行环球网
浏览器
40


SALOMON SMITH BARNEY
access
Site Links
Main Areas
Get Started
Register
Apply for Online Account Access
Site Tour
Get Information
Watch List
Quotes
Research Up/Downgrades
Marketwatch
Investor Education
Search/Sitemap
Branches & Seminars
your portfolio
investment ideas
financial planning
bill payment

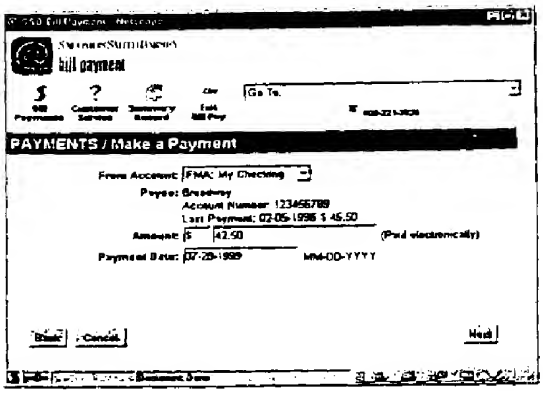

bill payment
PAYMENTS / Make a Payment
From Account:
Payee:
Amount:
Payment Date:
Next

图 3

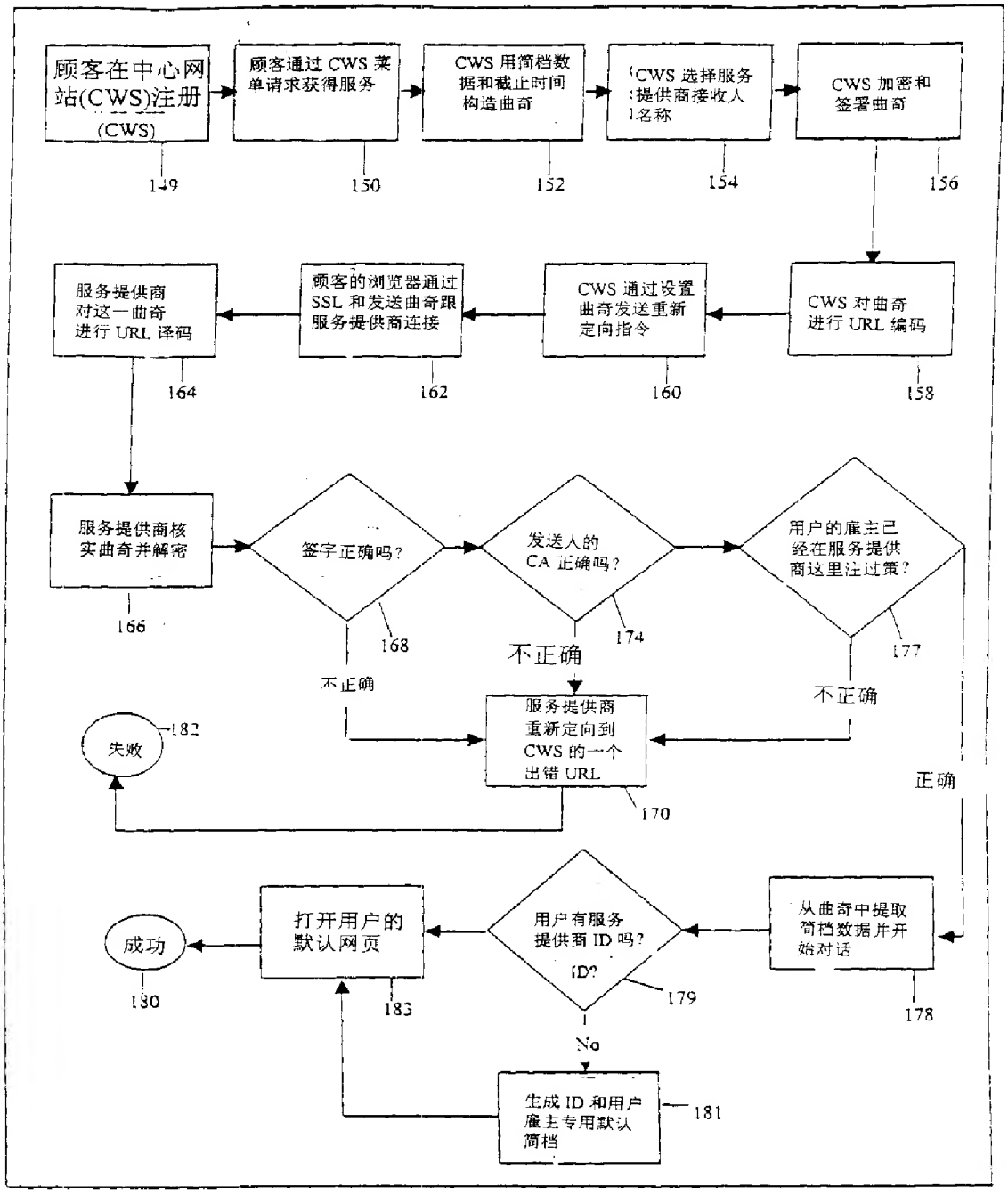

顾客在中心网站(CWS)注册
(CWS)
149
顾客通过 CWS 菜单请求获得服务
150
CWS 用简档数据和截止时间构造曲奇
152
CWS 选择服务提供商接收人名称
154
CWS 加密和签署曲奇
156
CWS 对曲奇进行 URL 编码
158
CWS 通过设置曲奇发送重新定向指令
160
顾客的浏览器通过 SSL 和发送曲奇跟服务提供商连接
162
服务提供商对这一曲奇进行 URL 译码
164
服务提供商核实曲奇并解密
166
签字正确吗?
168
不正确
发送人的 CA 正确吗?
174
不正确
用户的雇主已经在服务提供商这里注过策?
177
不正确
正确
服务提供商重新定向到 CWS 的一个出错 URL
170
失败
182
从曲奇中提取简档数据并开始对话
178
用户有服务提供商 ID 吗?
ID?
179
No
生成 ID 和用户雇主专用默认简档
181
打开用户的默认网页
183
成功
180

图 4